



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/920,919	08/02/2001	Kaijun Tan	230074-0238	7139
26694	7590	01/31/2006	EXAMINER	
VENABLE LLP			HOSSAIN, TANIM M	
P.O. BOX 34385			ART UNIT	
WASHINGTON, DC 20045-9998			PAPER NUMBER	

2145

DATE MAILED: 01/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 09/920,919	<b>Applicant(s)</b> TAN ET AL.	
	<b>Examiner</b> Tanim Hossain	<b>Art Unit</b> 2145	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 14 November 2005.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-27 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-27 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)             | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)    | Paper No(s)/Mail Date. _____  |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____   | 6) <input type="checkbox"/> Other: _____                                    |

## **DETAILED ACTION**

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vishwanath (U.S. 2005/0149759) in view of Cooper (U.S. 2001/0051996).

As per claim 1, Vishwanath teaches a method for distributing data over a network comprising: issuing a certificate and a private key to a client for identifying the client in a transaction (paragraph 0702); storing the certificate and the private key in a portable token of the client and used by the client during a transaction, the portable token being a physical device (0702, figure 13); verifying a digital signature using the certificate stored in the token before distributing data to the client (0702, 0515); and distributing the data to the client (Abstract). Vishwanath does not specifically teach the generation of a message associated with the data being downloaded. Cooper teaches the generation and sending of a message associated with the data being downloaded to the client and associated with the token used by the client during a transaction (paragraphs 0082, 0102). It would have been obvious to one of ordinary skill in the art at the time of the invention to include the generation of a message with token data into the distribution of content, as taught by Cooper in the system of Vishwanath. The motivation for

doing so lies in the fact that having a message with the token data would allow for better identification of the content to judge whether the correct content is being transmitted, for example. Both inventions are also from the same field of endeavor, namely the safe and secure transmission of media content through a network.

As per claim 2, Vishwanath-Cooper teaches the method of claim 1, further comprising providing the client with information necessary for establishing an account (Cooper: page 8, paragraph 0126).

As per claim 3, Vishwanath-Cooper teaches the method of claim 2, further comprising providing the client with the token (Vishwanath: 0702).

As per claim 4, Vishwanath-Cooper teaches a method for distributing data over a network comprising: establishing a secure connection between a client and a server (Vishwanath: 0702); issuing a certificate and a private key to the client for identifying the client in a transaction (Vishwanath: 0702); storing the certificate and the private key in a portable token of the client and used by the client during a transaction, the portable token being in a physical device; and generating a message associated with the data being distributed to the client and associated with the token used by the client during a transaction (Cooper: 0082, 0102).

As per claim 5, Vishwanath-Cooper teaches the method of claim 4, further comprising distributing data to the client (Cooper: page 2, paragraph 0019).

As per claim 6, Vishwanath-Cooper teaches the method of claim 5, further comprising requesting information from the client for establishing an account (Cooper: page 8, paragraph 0126).

As per claim 7, Vishwanath-Cooper teaches the method of claim 4, wherein establishing a secure connection comprises establishing a secure connection using a security protocol (Cooper: page 2, paragraph 0032).

As per claim 8, Vishwanath-Cooper teaches the method of claim 7, wherein the security protocol is the secure socket layer protocol (Cooper: page 2, paragraph 0032).

As per claim 9, Vishwanath-Cooper teaches the method of claim 6, wherein the requesting information comprises requesting a credit card number (Cooper: page 8, paragraph 0126).

As per claim 10, Vishwanath-Cooper teaches the method of claim 6, wherein requesting information comprises requesting a password (Cooper: page 8, paragraph 0126).

As per claim 11, Vishwanath-Cooper teaches the method of claim 4, wherein storing the certificate comprises: interfacing the token to a client computer (Cooper: page 1, paragraph 0018; page 2, paragraph 0042); and writing the certificate and the private key to the token across the network (Cooper: page 2, paragraph 0043).

As per claim 12, Vishwanath-Cooper teaches the method of claim 4, wherein storing the certificate comprises: interfacing the token to a server computer (Cooper: page 2, paragraph 0042); and writing the certificate to the token at the server computer (Cooper: page 5, paragraph 0064).

As per claim 13, Vishwanath-Cooper teaches the method of claim 5, wherein distributing data to the client comprises distributing a media player (Cooper: page 12, paragraph 0179).

As per claim 14, Vishwanath-Cooper teaches a method for distributing data over a network comprising: establishing a secure connection between a client and a server

(Vishwanath: 0702; Cooper: page 2, paragraph 0032); receiving a request from the client for data to be downloaded (Vishwanath: 0702; Cooper: page 2, paragraph 0019); generating a message associated with the data being downloaded to the client and associated with a portable token of the client and used by the client, the portable token being a physical device (Vishwanath: 0702; Cooper: page 8, paragraph 0102); and distributing the data and the associated message to the client (Cooper: page 8, paragraph 0110).

As per claim 15, Vishwanath-Cooper teaches the method of claim 14, wherein establishing a secure connection comprises establishing a secure connection using a security protocol (Cooper: page 2, paragraph 0032).

As per claim 16, Vishwanath-Cooper teaches the method of claim 15, wherein the security protocol is the secure socket layer protocol (Cooper: page 2, paragraph 0032).

As per claim 17, Vishwanath-Cooper teaches the method of claim 14, wherein establishing a secure connection comprises requesting authentication information from the client (Cooper: page 8, paragraph 0126); and sending authentication information from the server (Cooper: page 5, paragraph 0057).

As per claim 18, Vishwanath-Cooper teaches the method of claim 17, wherein requesting authentication information from the client comprises requesting a certificate from the client (Cooper: page 2, paragraph 0018); and requesting a digital signature from the client (Cooper: page 5, paragraph 0057; where the retrieving of a digital certificate includes the digital signature).

As per claim 19, Vishwanath-Cooper teaches the method of claim 17, wherein sending authentication information from the server comprises sending a certificate from the server; and sending a digital signature from the server (Cooper: page 14, paragraphs 205-209).

As per claim 20, Vishwanath-Cooper teaches the method of claim 18, wherein requesting a certificate comprises reading the certificate from the token used by the client (Cooper: page 11, paragraph 0163).

As per claim 21, Vishwanath-Cooper teaches the method of claim 14, wherein generating a message further comprises: including in the message a data identification number (Cooper: page 5, paragraph 0060, page 6, paragraph 0075, and page 8, paragraph 0102; where the watermark contains the identification number and message); including in the message a period of time for which the data may be used by the client (Vishwanath: 0105); including in the message a distinguishing number of the token used by the client when requesting data (Cooper: page 5, paragraph 0060, page 6, paragraph 0075, and page 8, paragraph 0102); and including in the message a symmetrical key used to encrypt the data from the server to the client over the network (Cooper: page 5, paragraph 0060, page 6, paragraph 0075, and page 8, paragraph 0102). Motivations to combine teachings are discussed in the treatment of claim 1.

As per claim 22, Vishwanath-Cooper teaches the method of claim 14, wherein generating a message further comprises generating a message using a public key (asymmetric) cryptographic algorithm (Cooper: page 8, paragraph 0103).

As per claim 23, Vishwanath-Cooper teaches a method of securely utilizing downloaded data comprising: opening a media player (Cooper: page 8, paragraph 0124); opening a data file (Cooper: page 8, paragraph 0124); requesting a portable token from and used by a client, the

portable token being a physical device (Cooper: page 2, paragraph 0018; Vishwanath: 0702); reading a distinguishing number from the token (Cooper: page 5, paragraph 0060, page 6, paragraph 0075, and page 8, paragraph 0102); verifying a digital message associated with the data file and the token using the media player, the distinguishing number, and a private key in the token (Cooper: page 5, paragraph 0060, page 6, paragraph 0075, and page 8, paragraph 0102).

As per claim 24, Vishwanath-Cooper teaches the method of claim 23, wherein in verifying a digital message, the media player reads the private key from the token to decrypt the digital message (Cooper: page 3, paragraph 0043).

As per claim 25, Vishwanath-Cooper teaches the method of claim 23, wherein in verifying a digital message, the media player sends the digital message to the token (Cooper: page 5, paragraph 0060, page 6, paragraph 0075, and page 8, paragraph 0102; where the whole watermarking process entails verification).

As per claim 26, Vishwanath-Cooper teaches the method of claim 25 and the use of a public key to decrypt an encrypted symmetric key, but does not specifically teach the token's decryption of an encrypted symmetric key using the private key. It would have been obvious to one of ordinary skill in the art at the time of the invention to include the functionality of the use of a private key to decrypt an encrypted symmetric key, as it is well known in the art. (See: Fischer, U.S. 5,436,972; column 12, lines 36-45, for example). Also, the use of a private key to decrypt, over the use of a public key is a design choice, and is thus not patentably distinct.

As per claim 27, Vishwanath-Cooper teaches the method of claim 23, wherein verifying a digital message comprises verifying the distinguishing number read from the token (Cooper:



page 5, paragraph 0060, page 6, paragraph 0075, and page 8, paragraph 0102); verifying a time period associated with the data file (Vishwanath: 0105); decrypting an encrypted symmetrical key using the private key from the token; and decrypting the data file using the symmetrical key (see discussion of claim 26).

### *Conclusion*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tanim Hossain whose telephone number is 571/272-3881. The examiner can normally be reached on 8:30 am - 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jason Cardone can be reached on 571/272-3933. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Tanim Hossain  
Patent Examiner  
Art Unit 2145

  
JASON CARDONE  
SUPERVISORY PATENT EXAMINER